1. A method comprising:

determining a private network address for a user in connection with the user accessing a network resource;

determining an access control list entry for the user based on an access control policy;

translating a public network address to the private network address for the user accessing the network resource; and

allowing or blocking the user access based on the access control list entry,

wherein determining the access control list entry is performed before translating the public network address to the private network address.

2. The method of claim 1, further comprising sending the determined access control list entry from a first computer on the network to a second computer on the network before allowing or blocking the user access.

3. The method of claim 2, further comprising:

generating an access control list entry corresponding to the access control policy, that entry including the determined private network address.

4. The method of claim 3, wherein the generated access control list entry comprises a network level access control list including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined network address, and an indication of allowed or denied access to the network resource.

5. The method of claim 2, wherein the determined access control list entry comprises an application level access control list entry stored on storage device connected to the first computer.

6. The method of claim 3, wherein determining the network address comprises allocating a network address based on a dynamic host configuration protocol (DHCP).

7. The method of claim 3, wherein the second computer comprises a network layer device, and

wherein blocking or allowing access comprises blocking or allowing access at the network layer device.

8. The method of claim 5, wherein the second computer comprises a server computer associated with the network resource,

wherein determining an access control list further comprises retrieving an application layer access control list entry stored in a database, and

wherein the server computer uses an application layer protocol based on an open system interconnection (OSI) model.

9. The method of claim 5, further comprising storing the access control policy on a storage medium connected to the first computer in the network, the access control policy including defined roles for each user allowed to access a resource in the network.

10. The method of claim 3, further comprising:

releasing the private network address following completion of the access to the network resource.

11. The method of claim 10, further comprising:

de-installing a network layer access control entry following completion of the access to the network resource.

12. An article comprising a machine-readable medium that stores machine-executable instructions, the instructions causing a machine to:

determine a private network address for a user in connection with the user accessing a network resource;

determine an access control list entry for the user based on an access control policy;

translate a public network address to the private network address for the user accessing the network resource; and

allow or block the user access based on the access control list entry,

wherein determining the access control list entry is performed before translating the public network address to the private network address.

13. The article of claim 12, further comprising instructions causing a machine to:

send the determined access control list entry from a first computer on the network to a second computer on the network before allowing or blocking the user access.

14. The article of claim 13, further comprising instructions causing a machine to:

generate an access control list entry corresponding to the access control policy, that entry including the determined private network address.

15. The article of claim 14, wherein the generated access control list entry comprises a network level access control list including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined network address, and an indication of allowed or denied access to the network resource.

16. The article of claim 13, wherein the determined access control list entry comprises an application level access control list entry stored on storage device connected to the first computer.

17. The article of claim 14, wherein determining the network address comprises allocating a network address based on a dynamic host configuration protocol (DHCP).

18. The article of claim 14, wherein the second computer comprises a network layer device, and

wherein blocking or allowing access comprises blocking or allowing access at the network layer device.

19. The article of claim 16, wherein the second computer comprises a server computer associated with the network resource,

wherein determining an access control list further comprises retrieving an application layer access control list entry stored in a database, and

wherein the server computer uses an application layer protocol based on an open system interconnection (OSI) model.

20. The article of claim 16, further comprising storing the access control policy on a storage medium connected to the first computer in the network, the access control policy including defined roles for each user allowed to access a resource in the network.

21. The article of claim 14, further comprising:

releasing the private network address following completion of the access to the network resource.

22. The article of claim 21, further comprising:

de-installing a network layer access control entry following completion of the access to the network resource.

23. An apparatus comprising:

a first memory that stores executable instructions; and

a first processor that executes the instructions from the first memory to:

determine a private network address for a user in connection with the user accessing a network resource;

determine an access control list entry for the user based on an access control policy;

translate a public network address to the private network address for the user accessing the network resource; and

allow or block the user access based on the access control list entry,

wherein determining the access control list entry is performed before translating the public network address to the private network address.

24. The apparatus of claim 23, further comprising:

a second processor connected to the first processor, wherein the first processor executes instructions to:

send the determined access control list entry from the first processor to the second processor in a network.

25. The apparatus of claim 24, wherein the first processor executes instructions to:

generate an access control list entry corresponding to the access control policy, that entry including the determined private network address.

26. The apparatus of claim 25, wherein the determined access control list entry comprises a network level access control list entry including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined network address, and an indication of allowed or denied access to the network resource.

27. The apparatus of claim 25, wherein determining the network address comprises assigning a network address based on a dynamic host configuration protocol (DHCP).

28. The apparatus of claim 25, further comprising:

a storage medium connected to the first processor, wherein the determined access control list entry comprises an application level access control list stored on the storage medium.

29. The apparatus of claim 24, wherein the second processor comprises a network layer device.

30. The apparatus of claim 29, wherein the network layer device executes instructions to block or allow access to the network resource based on the network level access control list entry.